REMARKS

The present Amendment cancels claims 1-10 and adds claims 11-23. Therefore, the present application has pending claims 11-23.

35 U.S.C. §103(a) Rejections

Claims 1-10 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Japanese Application Publication No. 11-289329 to Naor, et al. ("Naor") in view of U.S. Patent No. 5,867,578 to Brickell, et al. ("Brickell"). As indicated above, claims 1-10 were cancelled. Therefore, this rejection with respect to claims 1-10 is rendered moot. Applicants submit that the features of the present invention, as now more clearly recited in claims 11-23, are not taught or suggested by Naor or Brickell, whether taken individually, or in combination with each other as suggested by the Examiner, or in combination with any of the other references of record.

New claims 11-23 were added so as to more clearly describe the features of the present invention. Specifically, the claims were amended to more clearly describe that the present invention is directed to a method for authenticating a public key certificate, where the validity of the public key certificate is authenticated by a computer, as recited, for example in claim 11.

The present invention as recited in claim 11 provides a method for authenticating a public key certificate, where the validity of the public key certificate is authenticated by a computer. The computer executes a step of searching a path between any certification authority at a start point (a start certification authority) and at least one terminal certification authority. The terminal certification authority issues

the public key certificate to terminals. The computer also executes the steps of verifying the searched path, registering the verified path in a database, receiving a request to authenticate the public key certificate, and validating the public key certificate issued by the at least one terminal certification authority by using information relating to the verified paths registered in the database.

The above described features of the present invention are an improvement over the prior art. As described on page 1, line 5 to page 5, line 11 of the present application, the prior art includes a plurality of certificate authorities and an end entity that requests the authentication of validity of a certificate issued by a certificate authority not yet trusted by the end entity. In this circumstance, it is necessary to verify a plurality of certificates issued by the plurality of certificate authorities to confirm that the certificate issued by the not yet trusted certificate authority is valid. This prior art authentication process is time consuming, and therefore is problematic. The object of the present invention is to reduce the time taken from the time when an end entity requests authentication of a public key certificate until the time the certificate is authenticated.

The above described features of the present invention, now more clearly recited in the claims, are not taught or suggested by any of the references of record. More specifically, the features are not taught or suggested by either Naor or Brickell, whether taken individually or in combination with each other.

Naor discloses a method of authenticating items and a method of modifying a search authenticated tree. However, there is no teaching or suggestion in Naor of the certificate validity authentication method as recited in the claims.

In contrast to the above described object of the present invention, the object of Naor is to reduce the time taken for an authentication authority to issue expiration information of a certificate (i.e., whether a certificate is effective or has expired). To accomplish this object, Naor includes the use of conventional authentication trees and conventional search trees, where an authentication tree is superimposed onto a search tree, forming a search authenticated tree. The method of authenticating items includes authenticating membership or non-membership of at least one item in a set by computing an authentication path formed between the at least one item and a root. The method of modifying a search authenticated tree includes updating the search tree so as to obtain updated nodes, computing an authentication path formed by the updated nodes, and authenticating at least the root modified node by a digital signature.

The certificate validity authentication method of the present invention includes steps executed by a computer, which are quite different from the teachings of Naor.

For example, the present invention discloses searching a path, where the path is between a start certification authority and a terminal certification authority. Naor does disclose a path as in the present invention. As shown in Figs. 2A and 2B of Naor, the path does not include a start certification authority and a terminal certification authority. Instead, Figs. 2A and 2B illustrate: the leaves of a tree, where

the leaves are a certificate revocation list holding invalidated or revoked items (page 25, lines 1-3); internal nodes directly connected to the leaves; and the root of the tree, connected to the internal nodes. As described on page 15, lines 1-3 of Naor, the certification authority authenticates the tree by authenticating the root. In this way, Naor does not disclose a path as recited in the claim 11.

By way of further example, because Naor does not disclose a path as claimed, Naor further does not disclose the steps of: searching the path; verifying the searched path; registering the verified path; and validating a public key certificate by using information relating to the verified path registered in the database.

By way of even further example, the present invention discloses a step of receiving a request to authenticate a public key certificate. The method further includes validating a public key certificate issued by at least one terminal certification authority by using information relating to the verified paths registered in the database. Naor's method does not include validating the public key certificate using information relating to the verified paths registered in the database, as claimed.

Therefore, Naor fails to teach or suggest "a path search step of searching a path between any certification authority as a start point (a start certification authority) and a terminal certification authority which issues the public key certificate to terminals" as recited in the claims.

Further, Naor fails to teach or suggest "a path verification step of verifying the path searched by the path searching step" as recited in the claims.

Even further, Naor fails to teach or suggest "a path registration step of registering the path verified by the path verification step in a database" as recited in the claims.

Furthermore, Naor fails to teach or suggest "a validity authentication step of receiving a request to authenticate the public key certificate and validating the public key certificate issued by the at least one terminal certification authority by using information on the verified paths registered in the database" as recited in the claims.

The above noted deficiencies of Naor are not supplied by any of the other references, particularly Brickell, et al. ("Brickell"). Therefore, combining the teachings of Brickell with Naor still fails to teach or suggest the features of the present invention as now more clearly recited in the claims.

In contrast to the above described object of the present invention, the object of Brickell is to manage the key of the authentication authority. To accomplish this object, Brickell teaches multi-step digital signature system and method having a distributed root certifying authority. As shown in Fig. 1, messages are received at the root certifying authority (item 20) and are distributed to root certifying authority members (items 22-30). The root certifying members attach partial signatures to the messages using root key fragments. The Brickell system adapts to system events, such as the addition or removal of key fragment holders or the need to modify key fragments, by changing key fragments.

As recited in claim 11, the present invention includes registering a verified path in a database. Unlike the present invention, Brickell does not teach or suggest

registering a verified path in a database. There is no disclosure of a database or any other type of storage that registers a verified path.

In addition, Brickell does not teach or suggest authenticating the validity of a public key certificate issued by at least one terminal certification authority by using information relating to the verified paths registered in the database, as claimed. In the present invention, information relating to the verified paths in the database is used to validate the public key certificate issued by the terminal certification authority. Brickell does not disclose this feature.

Therefore, Brickell fails to teach or suggest "a path registration step of registering the path verified by the path verification step in a database" as recited in the claims.

Furthermore, Brickell fails to teach or suggest "a validity authentication step of receiving a request to authenticate the public key certificate and validating the public key certificate issued by the at least one terminal certification authority by using information on the verified paths registered in the database" as recited in the claims.

Naor and Brickell suffer common deficiencies relative to the features of the present invention as recited in the claims. Therefore, combining the teachings of Naor and Brickell would not render obvious the features of the present invention as now more clearly recited in the claims.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to Naor and Brickell.

In view of the foregoing amendments and remarks, Applicants submit that claims 11-23 are in condition for allowance. Accordingly, early allowance of such claims is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Mattingly, Stanger, Malur & Brundidge, P.C., Deposit Account No. 50-1417 (referencing attorney docket no. 566.40596X00).

Respectfully submitted,
MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Carl I. Brundidge
Registration No. 29,621

CIB/sdb
(703) 684-1120